Hendry County Sheriff's Office

General Order 5.8

TITLE: Internet Terms and Conditions	**SHERIFF'S APPROVAL:** Digital
ORIGINATION DATE: August 5, 2018	**REVISION DATE:** May 7, 2019
RELATED REFERENCES: *Department of Justice Criminal Information Services Security Policy, §119 F.S.* **CFA:** *26.04M, 32.01*	
REVIEW FREQUENCY: 3 YEARS	**DATE OF NEXT REVIEW:** May 7, 2022

I. PURPOSE: The purpose of this order is to ensure that agency members understand the terms and conditions of internet usage when using the agency's network.

II. SCOPE: This order shall apply to all sheriff's office members.

III. POLICY: The Hendry County Sheriff's Office standardized communication systems are to assist in business operations of the agency and is not for personal use.

IV. PROCEDURE:

A. ACCEPTABLE USE CONDITIONS

1. The purpose of the Smartcop system and Internet access is to provide the law enforcement community with unique resources and the opportunity for collaborative work.

2. The utilization of a user account must be in support of law enforcement, associated research and administrative functions, and must be consistent with the objectives of the Hendry County Sheriff's Office and associated law enforcement agencies.

3. Use of other organization's networks or computer resources must comply with the rules appropriate for that network or system.

4. Publication, ownership or transmission of any material in violation of any U.S., state or local regulation is prohibited. This includes, but is not limited to: copyrighted material, threatening or obscene material, or material protected by trade secret.

5. All communications and information accessible via the network should be considered the property of the information source whether local, state, federal or public.

6. Use of the Sheriff's computer or network for product advertising (except personal advertising on the Sheriff's bulletin board) or political lobbying is prohibited.

7. All communication must use appropriate and professional language.

8. Electronic mail in the Sheriff's e-mail server and the Internet has no expectation of privacy and can be reviewed without notification to the user.

9. Although all e-mail transmissions and arrivals are automatically archived for a 3-year period, it is the responsibility of the end user to review and understand Florida public records law and to make arrangements to retain e-mails for longer periods.

10. Internet activities that are not permitted include:

    a. Copying, saving or redistributing copyrighted material

    b. Subscribing to any services unless approved by the Sheriff or designee

    c. Sharing of any other user information such as address and phone number

    d. Playing games or using other interactive sites such as chats, unless specifically assigned by the Sheriff or designee

    e. Use of the network in such a way that you disrupt the use of the network by other users

    f. Creation and/or distribution of computer malware on any computer in the network

    g. Downloading any unauthorized software or copyrighted material

    h. Any activity that violates a Sheriff's Office policy, local, state or federal laws, or any interference with network, anti-virus or other computer security measures.

11. Any user who may have questions or doubts concerning a specific activity's permissibility should contact the Information Technology Unit (ITU) prior to execution.

12. Authorization for access to the network will be established by the ITU exclusively wherein no standard user may add or remove access privileges assigned to other users.

13. Outside agency information services and shared data resources are also governed by this Procedure. All access, use and dissemination of criminal justice and personally identifiable information shall be in accordance with the current FBI CJIS Security Policy. Any illegal or unauthorized activities concerning the retrieval of criminal justice and personally identifiable information such as warrant, criminal histories, NLETS, FCIC/NCIC, CJNET and DHSMV data will result in account termination and may produce civil and/or criminal prosecution.

14. This Procedure is further governed by Department of Justice Security Policy CJISD-ITS-DOC-08140-5.0.

B. Privileges

1. The use of the Sheriff's computer system and network is a privilege, not a right, and inappropriate use can result in cancellation of those privileges.

    a. Based upon the acceptable use guidelines outlined in this Procedure, the system administrator will deem what is inappropriate use of the network and take appropriate action.

b. The system administrators may recommend suspension or closure of an account to the Chief Deputy at any time as required.

c. Only the Sheriff or the Chief Deputy may authorize re-establishment of an account.

d. Terminated users will be notified in writing by the ITU within two weeks of the termination, and the notice will include the reason for the account termination.

e. Accounts which have been terminated or access denied do have the following rights:

(1) To request in writing a written statement justifying the actions

(2) To submit a written appeal to the ITU, as a follow-up to this letter, in order to have a meeting with the staff of the ITU, their command supervisor and the Chief Deputy.

f. The ITU will conduct an annual audit of the central records computer system. This audit will provide for the verification of the following: all passwords, access codes, and access violations.

C. Publication of Materials

1. Publication of any material, including e-mail and Web content, should have the author's name and e-mail address.

2. Employees must obtain approval from the Sheriff or the Chief Deputy to post content on Web sites associated with the Sheriff's Office.

3. The Sheriff or the Chief Deputy must approve all content changes to the Sheriff's Office Internet Web site, with the exception of routine updating.

4. No copyrighted materials may be used without the owner's consent; this includes photographs, cartoons and logos.

D. Security

1. Network security is a high priority.

a. Any security problems on the Sheriff's computer network should be provided to the Information Technology Unit (ITU) or the Chief Deputy, and should not be demonstrated to other users.

b. A user may not under any circumstances use another individual's account.

c. A user cannot give their password to any other individual.

d. Attempts to log in to the Sheriff's computer system or network as a systems administrator will result in immediate termination of the user account.

e. Authorized users may view criminal history information automated in Smartcop. An automated log of all criminal history records printed is maintained by the ITU. Criminal history information contained in Smartcop may only be disseminated to other law enforcement agencies. No Smartcop user will disseminate or provide criminal history information to non-law enforcement persons. Any non-law enforcement request for criminal

history information will be forwarded to the Sheriff's Records Unit as a public records request.

f. Users shall not add or remove access privileges assigned to other users.

E. Vandalism

1. Vandalism may result in cancellation of privileges.

2. Vandalism is defined as any attempt to obtain, harm, or destroy data of another user, the Sheriff's computer or network, or any other network or workstation that is connected to the Internet or intranet backbone. This includes, but is not limited to, the uploading or creation of computer viruses.

F. Reliability

1. The Sheriff's Office makes no warranties of any kind, whether expressed or implied, for the service it is providing.

2. The Sheriff's Office will not be responsible for any damages a user may suffer; this includes loss of data resulting from delays, non-deliveries, incorrect deliveries, or service interruptions caused by its own negligence or a user's errors or omissions.

3. Use of any information obtained via the Sheriff's computer and network is at the user's own risk.

4. The Sheriff specifically denies any responsibility for the accuracy or quality of information obtained through its computer network services.

G. Indemnity

1. The user specifically agrees to indemnify the Sheriff or any of its employees for any losses, costs, or damages, including reasonable attorneys' fees incurred by the Sheriff and employees relating to, or arising out of, any breach of this policy.

H. Exception of Terms and Conditions

1. All terms and conditions as stated in this document are applicable to the Sheriff's Office and all subscribers. These terms and conditions reflect the entire agreement of the parties and supersede all prior oral or written agreements and understandings of the parties. These terms and conditions will be governed and interpreted in accordance with the laws of the State of Florida.

I. Software and Hardware Restrictions

1. No software will be deleted, modified or loaded onto any workstation that is the property of the Sheriff without written authorization of the Information Technology Unit (ITU).

2. Any workstation that has been altered without the express permission of the ITU will require the workstation to be returned to the ITU until the workstation can be returned to a known working state.

3. Any costs incurred to return the workstation to a legal configuration, including man-hours exhausted, may be charged to the unit or cost center recommended by the ITU.

4. Access to the network will be established by the ITU exclusively wherein no standard user may add or remove access privileges assigned to other users.

V. GLOSSARY

COMPUTER EQUIPMENT – Any device used to create, store, exchange or utilize data.

ELECTRONIC MAIL (E-MAIL) – Electronic transmission medium for messages, documents, and other forms of correspondence. E-mail is not considered a record series or category.

INTERNET – Worldwide Network established by the Department of Defense Advanced Research Projects Agency for the purpose of information interchange.

NETWORK – Protocol by which personal workstations are connected to a host server and other workstations within the existing LAN.

PUBLIC RECORDS – Section 119.011(1), F.S., defines public records as:
"All documents, papers, letters, maps, books, tapes, photographs, films, sound recordings, data processing software, or other material, regardless of physical form, characteristics or means of transmission, made or received pursuant to law or ordinance or in connection with the transaction of official business by any agency".
Examples of public records include intra-office memoranda, and preliminary working drafts communicated to other members of the Sheriff's Office for review. When in doubt as to whether your E-mail is a public record consult the Sheriff's Records Unit Manager.

SYSTEMS ADMINISTRATOR – Any person charged with the maintenance, deployment and user support of Information Management System or its components.

VANDALISM – Willful and/or malicious destruction, disfiguring or assault upon property not belonging to the perpetuator of the activity.

Your electronic signature in Power DMS acknowledges you have read this policy and understand it.